UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/287,924	04/07/1999	RYUJI ISHIGURO	450100-3689.	6867

20999 7590 08/02/2004

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
SEAL, JAMES	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 08/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/287,924	ISHIGURO ET AL.	
	Examiner	Art Unit	
	James Seal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *60-95* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *60-95* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. 8.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's correspondence of 30 April 2004.

2. Amended claims have been entered.

3. Claims 60-95 are pending.

Specification

4. The new title "Location Dependent Key for Decrypting Copy Protected Material On A Recording Medium is acceptable and has been entered.

5. New Abstract is acceptable and has been entered.

Claim Objections

6. With the amendment to claims 74-75, 81-82, 86, 88, and 93-94 the examiner withdraws his object.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 60-64, 84-85, 89-92 and 95 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis US 5596639 A, and further in view of Davis et. al. Cryptographic Randomness from Air Turbulence in Disk Drive and Adler US 3985952 A.

8. As per claim 60, the limitation of encrypting data and recording the data on a recording medium (compact disk) is disclosed by Kikinis (see Column 4, 50-54; Figure

3). The limitation of generating an encryption key which is based on information recorded to a predetermined region of the same surface is disclosed by Kikinis. Kikinis discloses figure 3 that the encryption key is derived from the password (key data) and that the password is stored are stored in area 37 of the surface (Column 4, lines 57-58). Kikinis further discloses that the encrypted data is store in region 35 of the disk (Column 4, line 49). Thus Kikinis teaches that the data for generating the encryption key (key data) is stored on the same surface of the disk, but in a different region of the same surface (region 37 versus region 35, see Figure 3). Kikinis does not state that the region in which the key data has been placed is a "predetermined region" and "determined from the recording medium" however this would be inherent from Figure 3 that region 37 is predetermined in that it lies radially outside the data storage region (area 35) and is thus determined from the recording medium's geometry (Column 4, line 55). Kikinis is silent on the generation of key material based on the wobbling frequency of the recording medium.

9. Davis et. al. teaches the extraction of random data using the variations in speed of a disk drive due to unpredictability of air turbulence for cryptographic use (See page 114 Introduction lines 6-8). In the statistical analysis using an IBM pc and and Micropolis hard disk they were able to generate random data at 100 bit/minutes. Further at this rate they suggest that they could generate 2600 highly random DES keys/day (page 118). Davis teaches using the natural variations in the speed of a rotating disk as a source of random number to in turn generate cryptographic keys. Although it would be apparent that this method could be applied to CD, Adler teaches a

method by which the disk wobble of an optical disk can be measured and thus obtain the timing data to implement Davis teachings. Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made that one could generate the random numbers necessary in Kikinis invention from the wobbling frequency of the CD taught in Adler applying the tecnique of Davis because as Davis points out it is low-cost, easily whitened, reliable and mathematically noisy (Introduction). Claim 60 is rejected.

10. Claim 61 is an apparatus implementation of method claim 60 (that is encrypted data on a recording medium) and is rejected in view of the same prior art of record.

11. Claim 62 recites the limitation of recording the encrypted information on the recording medium according to claim 60 and is rejected in view of the same prior art of record.

12. As per claim 63, the limitations that the recording key data includes wobble frequency and/or wobbled land portion of recording medium of disk is not disclosed by Kikinis. Davis page 114 teaches the use of random fluctuation occurring in hardware, such as air turbulence in a sealed disk drive, as a means of generating random numbers. Davis further teaches key generation using random fluctuation in mechanical devices Further Davis notes the need to replenish key material for cryptosystem such as DES and public keys (bottom page 118). Adler discloses the need for a beam wobbling device, which applies a known correction through a servo mechanism, to prevent the departure of the spot from its correct position on the record track (Column 1, 45-60). Such fluctuation would constitute random fluctuation of the type that Davis uses

for the generation of key material. Thus one of ordinary skill in the art at the time the invention was made would have been motivated to use the known random fluctuation in tracking as typified by Alder's discussion of the wobble frequency as a means to implement Davis generation of key material from such fluctuations, because such material are already available from the tracking using in a CD. Claim 63 is rejected.

13. As per claim 64, the limitation of storing information (e.g. wobble pre-groove data) in a data files used for program operations would have been obvious to one of ordinary skill in the art at the time of the invention because it would convent and save time of downloading material from other sources. Claim 64 is rejected.

14. As per claim 84, the limitations are the same as those of claim 60 with the except that the limitation that the encryption key is based on key data in claim 60 is replaced in claim 84 with encrypted key is based on data. Random data is one form of data and thus claim 84 is rejected in view of the same prior art of record as claim 60.

15. As per claim 85, the limitation of decrypted encrypted data stored on a recording medium is disclosed by Kikinis (see Abstract). Decrypting a first file which has encrypted data (Kikinis Figure 3 element 35) generating an encryption key based on information recorded in a predetermined region on the same surface yet is not part of the encrypted region (Kikinis, Figure 3, element 37) and then decrypting encrypted data. Claim 85 is rejected.

16. As per claim 89, the limitation of a recording medium (Kikinis Figure 3) with a storage area for storage (Kikinis, Figure 3, element 35) such that the recording medium has both encrypted data and random data on it (Kikinis stores the encrypted data Figure

3, element 35, and the random data (for example a key) in region 37), according to which the encryption key which is based on the random data (and indeed may be the random data) since if the keys are not random the encryption will be broken) and the random data is recorded on predetermined regions of the same surface (Kikinis Figure 3, element 37, Figure 5, Column 1, lines 44-46). Further note this claim would read the CSS encryption used in most CD copy protection today. Note nothing in this claim restricts the keys from being in the same or different areas. Claim 89 is rejected.

17. As per claim 90, the limitation that the random data is associated with predetermined is disclosed by Kikinis Figure 3, element 37. Claim 90 is rejected.

18. As per claim 91, the limitation that the encryption key is based on wobbling frequency see arguments with regard to claim 63. Claim 91 rejected.

19. As per claim 92, the limitation or one or more predetermined region see Kikinis Figure 5. Claim 92 is rejected.

20. As per 95, the limitation of a second encryption key and a third encryption key (see Kikinis Figure 5), that the encryption keys for say an AutoCAD program. One of ordinary skill in the art at the time the invention was made would have been motivated to add more keys to include different types of programs which would be produced by different vendors because different licensing or different copyright agreements. Claim 95 is rejected.

21. Claim 65-80, 83, 81-82, 86-88, and 93-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kikinis US 5596639 A as applied to claims 60-62 above, and further in view of Elmer et. al. US 5058164 A.

22. As per claim 65, the limitations of generating encrypted data and placing the encrypted data on recording medium and further generating an encryption key based on key data which is recorded to a predetermined region of the same surface determined from say recording medium yet not part of encrypted is disclosed by Kikinis and discussed in relation to claim 60. Kikinis is silent on the limitation that the key data depends upon random data which has been inserted in-between said encrypted data. Elmer teaching using bytes in a storage medium which are in-between other storage data for the purpose of generated key material Column 6 lines 50-54. The chosen bytes do not have values specially assigned for encryption, they are merely chosen, according to a rule, from the body of data to be encrypted. These bytes form a key which encrypt themselves and all of the remaining data surrounding them. Thus key material is interspersed with stored encrypted data. Elmer goes on to say that this method may be used in other forms of data encryption such as data transmission (Column 6, lines 36-40). Further, it would be the case that in data transmission the bits/bytes are not address and so the key data would have to be identified by position in the data stream. Further, as stream data does not necessitate blocks, one could drop the restriction to bytes of data. Thus Elmer teaches of any amount hiding key material within stored encrypted material. One of ordinary skill in the art at the time of the invention would have been motivated to use the teachings of Elmer with those of Kikinis, because

encrypted data (which is already random, otherwise it could be easily broken), to ideal to hid (or obfuscate) random key data (on which the key is generated) as you are in effect hiding random data in random data. Claim 65 is rejected.

23. As per claims 66, 75, 77, and 82, the limitation recording program information in files would have been obvious to one of ordinary skill in the art (see claim 64 for discussion). Claim 66, 75, 77, and 82 is rejected.

24. As per claims 67, 68, 69, 70, 71-72, and 78 the limitation of creating a file in compliance to a well known standard for file formatting on a CD (ISO9660) including interleaved files and multi extent files which has been long established (since 1988) and is disclosed by Kikinis (Column 2, line 54). Claims 67, 68, 69, 70, 71, 72, and 78 are rejected.

25. As per claim 73, wherein the random file data is recorded on a surface of said the recording medium is disclosed by the combination Kikinis/Elmer (Kikinis Column 1, lines 44-46; Column 2, lines 36-43). Claim 73 is rejected.

26. Claims 76-78 is an apparatus implementation of claim 65-67 and is rejected in view of the same prior art of record.

27. Claims 79-80 disclose a method of recording information on a recording medium with the same limitations as claims 65-66, in which the information to be recorded is encrypted information. Claims 79-80 are rejected.

28. As per claim 83, the limitation of creating a file in compliance to a well known standard for file formatting on a CD (ISO9660) including interleaved files and multi

extent files which has been long established (since 1988) and is disclosed by Kikinis (Column 2, line 54). Claim 83 is rejected.

29. Claim 87 is an apparatus for implementing method claim 79 and is rejected in view of the same prior art of record.

30. As per claim 74, the limitation that the random data is selected from a portion of a random file data. Elmer teaches using a portion of stored data, which would include stored files selected at random as key material. Claim 74 is rejected.

31. As per claim 86, the limitation of decrypting the encrypted data recorded on a recording medium with the encrypted key is based on key data from a portion of a random file located in a predetermined position of the surface but not with the encrypted data and such that the encrypted data is generated from a predetermined portion of a random file is disclosed by Kikinis/Elmer. Kikinis discloses the key data being stored in a file in a predetermined part of the surface 37 not part of the stored encrypted data, the key data used to determine the encryption key for decryption of the key data see figure 3 ad 5 and details above. Kikinis is silent on how the decryption key is generated from te key data but as the key must be a random number string it is inherent that at least part of the key data is the source of this random string and must be random. Elmer teaches the use of a portion of stored data such as a file as key material. Kikinis further teaches a plurality of key data see figure 5 so it would be inherent that only a portion of the file is used for generating encryption key. Thus one of ordinary skill in the art at the time that the invention was made would have been motivated to combine the data created with a pseudorandom data generator to generate a key string as dictated by a

portion of the key data file residing in a predetermined area 37 of the disk again for ease of generation of such numbers. Claim 86 is rejected.

32. Claim 88 is an apparatus claim for implementing method's claim 86 and is rejected in view of the same prior art of record.

33. As per claims 93-94, the limitation of a file generated by a pseudo random generator see arguments claim 74 and Kikinis Figure 3, element 37. Claims 93-94 are rejected.

Response to Arguments

Applicant's arguments with respect to claim 60-95 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

James Seal
Examiner AU-2135
24 July 2004